CYBERSECURITY: PRESSING PRIORITY IN INDIA

Dr. Khyati Tejpal, Assistant Professor
Global Business School and Research Centre
Dr. D.Y. Patil Vidyapeeth, Pimpri, Pune
khyatitejpal06@gmail.com

Dr. Jayashree Patole, Assistant Professor
Global Business School and Research Centre
Dr. D.Y. Patil Vidyapeeth, Pimpri, Pune
jayashree.patole@dpu.edu.in

Tanmay Ghugare, Student of MBA
Global Business School and Research Centre
Dr. D.Y. Patil Vidyapeeth, Pimpri, Pune
tanmayrghugare@gmail.com

ABSTRACT
This research paper aims to provide a comprehensive analysis of the current state of cybersecurity in India. The study begins by establishing a clear understanding of cybersecurity and its key elements, highlighting its significance in today's digital landscape. It then delves into the various cyber threats that individuals and organizations in India face on a regular basis, including phishing attacks, malware infiltrations, and data breaches, among others. To address these challenges, the report examines the proactive steps taken by the Indian administration. Additionally, the establishment of Computer Emergency Response teams plays a crucial role in rapidly responding to and mitigating cyber incidents. In conclusion, the paper emphasizes the growing need to strengthen cybersecurity measures in India. It highlights the importance of continuous efforts to improve cybersecurity education and awareness among individuals and organizations. Additionally, the research underscores the significance of developing a robust legal framework to address cybercrime effectively. The paper concludes by stressing the importance of collaboration with international organizations to effectively combat cyber threats in an interconnected world.
Keywords: Cybersecurity, cybercrime, legal framework, challenges, threats, methods, initiatives.

Introduction

In today's technologically advanced society, the growing reliance on technology has made cybercrime a significant problem. The rapid development of technology has transformed the way individuals interact with the world, with the internet becoming an integral part of daily life. It provides easy access to various services, such as social networking, online shopping, studying, and employment opportunities, among others. However, this increased connectivity and dependence on the internet have also given rise to new forms of criminal activity known as cybercrime.

Cybercrime stands apart from other types of crimes due to its unique characteristics. Unlike traditional crimes, cybercrime knows no territorial boundaries, and identifying the perpetrators can be extremely challenging. The anonymity provided by the digital realm poses a significant challenge for law enforcement agencies, businesses, and individuals affected by cybercrime. All segments of society, including the government, private enterprises, and citizens, bear the impact of cybercriminal activities. The country's rapid digitization and increased connectivity have created new opportunities for cybercriminals to exploit vulnerabilities in the digital infrastructure. As a result, it is crucial to examine the nature of cybercrime in India, its various forms, and the legal amendments made to address this evolving threat landscape.

Unlike traditional crimes, cybercrime transcends geographical borders and can be carried out remotely, making it a global threat. Criminals exploit vulnerabilities in computer systems and networks to gain unauthorized access, steal sensitive information, disrupt services, or cause financial harm. The anonymity and reach provided by the internet present unique challenges in identifying and apprehending cybercriminals. The impact of cybercrime is far-reaching, affecting individuals, businesses, governments, and society as a whole. For individuals, falling victim to cybercrime can lead to financial loss, identity theft, invasion of privacy, and emotional distress. In the business realm, cyberattacks can result in significant financial damage, reputational harm, and loss of customer trust.

Governments face the challenge of protecting critical infrastructure and sensitive information from cyber threats. The rapid advancement of technology, increasing connectivity, and the digitization of various sectors have contributed to the growth of cybercrime. As individuals and organizations become more reliant on digital platforms and store vast amounts of data online, the potential for cybercriminals to exploit vulnerabilities and launch attacks also increases.

To address the rising threat of cybercrime, governments around the world have implemented legislation and established specialized law enforcement units and cybersecurity agencies. These measures aim to deter cybercriminals, investigate cybercrimes, and ensure that perpetrators are held accountable for their actions. International cooperation and collaboration are also crucial in combating cybercrime, given its transnational nature. Furthermore, raising awareness about cyber risks, promoting cybersecurity best practices, and educating individuals and organizations about potential threats is vital in reducing vulnerabilities and enhancing resilience against cybercrime. By adopting robust cybersecurity measures, such as regularly updating software, using strong passwords, and implementing encryption and firewalls, individuals and businesses can significantly mitigate the risks posed by cybercriminals.

Cybercrime poses a significant and evolving threat in today's digital age.
Addrebreakthroughs, regulatory frameworks, international cooperation, and public awareness due to its borderle ss nature and potential for severe effects. By understanding the nature of cybercrime and taking proactive measures to protect ourselves and our digital infrastructure, we can strive toward a safer and more secure digital environment.

Objectives

1. To examine the current state of cybersecurity in India and identify the country's key threats.
2. To examine India's current cybersecurity policies and practices, including government and private sector initiatives.
3. To identify gaps in cybersecurity infrastructure in India and recommend strategies to address these gaps.

Review of Literature

Digital security integrates advancements, strategies, and practices intended to safeguard PCs, applications, organizations, and insights from hacking, hurt, or unapproved access. Digital security is likewise periodically conflated improperly in open conversation with different ideas along with privateness, records sharing, knowledge gathering, and observation. Digital security comes into the picture notwithstanding going over cybercrimes. To avoid giving cybercriminals the drive, it is vital for those stressed inside the battle against cybercrime to endeavour to expect subjective and quantitative changes in its hidden variables to suitably form their techniques (Dani, 2022).

In a blast opened by the public area Wrongdoing procedures division kept down (NCRB 2011), the rate of cybercrimes under the IT undertaking has more prominent than before by 85.4% in the day 2011 when contrasted with 2010 in India, everyplace the improvement in the frequency of the wrongdoing under IPC is by 18.5% when contrasted with the day 2010. Visakhapatnam procedures are the more prominent roof way to deal with of occurrence of cases. Maharashtra has arisen as the hub of cybercrime with an incomparable figure of the rate of enrolled packs under cybercrimes. Hacking with machine frameworks and vulgar soft cover where the main stuff under IT imagine for cybercrimes. more noteworthy direct guilty parties captured for cybercrimes were in the get huge gathering 18-30 years. 563 gathering in the pickup grown-up occur in show 18-30 vocations were captured in the day 2010 which had developed to 883 in the day 2011 (Chitra, n.d.).

According to a McAfee assessment, the annual cost to the global economy is estimated to be $445 billion; however, a Microsoft report demonstrates that such overview-based measures are "horrendously imperfect" and significantly overstate the true losses. Online fraud using credit and cheque cards cost the US about $1.5 billion in 2012. According to a Juniper Exploration study from 2016, the cost of cybercrime could reach 2.1 trillion dollars by 2019. The majority of cybercrimes focus on phishing, misrepresentation, and fraud. India is the third most designated country for phishing assault after the US and the UK (Hati, 2016).

In August 2018, two Mumbai residents were detained for cybercrime. They committed fraud, including money transfers from their bank accounts, by illegally obtaining the SIM card information of several persons. These swindlers were gathering information about victims, disabling their SIM cards later with the help of fake documentation, and then conducting online banking transactions. They were accused of shifting 4 crore Indian Rupees from various accounts with ease. They even made an attempt to hack into the accounts of several firms.

The con artists will do this by obtaining client information, such as name, phone number, and identification, from a business or from some public sourcesAfter that, they obtained the 4G sim card by giving the telecom firm the necessary details of consumers who are already using 3G sim cards along with their phone numbers, called the customer, and pretended to be a customer service representative. On the back of the 4G sim card, there will be a 20-digit number that needs to be entered by the customer in order to quickly activate the 4G sim card. Customers who do that will deactivate their 3G sim card and activate their 4G sim card. But 4G sim card is still with the fraudsters in which they will perform bank transactions and receive OTPs (Lakshmanan, 2019).
Additionally, criminality often coincides with political demands or objectives. Prosecutions based on the dissemination of terrorist messages or information online call into question the very foundation of our fundamental ideals because liberal democracy is predicated on the acceptance of free debate of political viewpoints. It is challenging to strike the right balance between protecting civil freedoms and thwarting threats to our societies, and this equilibrium is never secure. The States' inability to agree on a common definition of the offence, notwithstanding the adoption of a European definition, poses the first challenge. Logically, “cyber-crime” as a concept is greatly discussed. Some scholars argue that it should be limited to cyber-attacks carried out by terrorists whereas others contend that it should encompass all uses of the Internet for terrorist purposes (Mali, 2018).

In its developing digital economy, India has the second-highest client-based internet in the world. Cybercrime is the term for illegal computer usage. A new revolution in the world economy occurred in the new millennium with the transition from the physical to the digital sphere. While traditional crimes can be committed with or without the aid of a computer, cybercrimes encompass more specialised types of crimes like viruses and phishing scams. Cybercrime, sometimes known as "online crimes" or "computer crimes," refers to any illegal activity that makes use of the internet. Cybercrime is a relatively recent type of illegal behaviour. Any illegal action that occurs or is carried out on or through the use of computers, the internet, or any other technology recognised under the Information Technology Act is referred to as cybercrime. In India, cybercrime is the most pervasive and effective form of crime, and it has terrible consequences. Criminals not only cause devastated and long-term damages to society, but to the Government also, but they also conceal their identities to a large and substantial extent (Supriya, 2022).

Research Methodology

A research design outlines frames the exploration questions that will be inquired. It lays forward a sensible association of the estimating methods, test plan, scientific system, and time span. Descriptive research methodology was used for this study because this approach is utilized when the study's problem requires a thorough and in-depth explanation.

Data collection method: The technique used for gathering the data is secondary. To improve the overall effectiveness of the research, existing data is compiled and summarised. The data can be collected either by primary method or secondary method. The method used in this study is secondary.

Secondary Data Analysis

Cybercrime and its causes

‘Cybercrime' incorporates a wide number of acts, wrongdoings or unlawful direct executed by the two people or gatherings against PCs, PC related gadgets, or data innovation organizations, as well as customary violations that are worked with or kept up with by the utilization of the web or potentially data innovation (Phillips, 2022).
There are 5 common trends that give chances to cybercrime:

1. An increase in online transactions and digital data. Product launch outcomes, client and transaction figures, and other market information are easily available. Online intellectual property creation is a desirable goal.
2. In comparison to the past, businesses and organisations are required to be more transparent. Most people want to be able to use their mobile devices to access business networks for daily chores. Smarter technology products can present the most current security threats even as they improve connectivity. Hackers may be able to bypass these security procedures, giving them instant access to corporate networks.
3. Viral-like software and malicious spyware are potent enough to partially control important programmes.
4. Businesses link their customers and suppliers to networks to increase business profits. Numerous people posing as members of the unidentified gang attacked a well-known e-commerce business in December 2010. In retaliation for the website ceasing to offer payment services to other websites, they attempted to launch a "denial-of-service attack." For the offense, more than a dozen hackers were detained.

5. Professional hacking groups and organizations are advancing in terms of technology. For example, a hacker might receive payment to put malware on end-user devices. Modern malware is difficult to detect and steals data for financial gain. Some people think that becoming hackers will allow them to make more money than working in security.

Cybersecurity

Computers, networks, data, and other digital assets are protected from unauthorised access, theft, damage, and other hostile actions by means of practises, processes, and technology known as cybersecurity.

It involves a number of procedures and techniques aimed at preserving the confidentiality, veracity, and usability of data and information systems. Cybersecurity is essential for individuals, businesses, governments, and other organisations that utilise digital technology to store, process, and transport sensitive information. It covers a variety of subfields, including network security, application security, information security, cloud security, and others.

1. Application Security: Application security, the first and most crucial component of cyber security, incorporates security elements inside programmes during the development phase to thwart cyberattacks. It defends against a range of cyber security attacks that use source code defects to harm websites and online software.
2. Information Security: The element of cyber security that deals with measures to thwart unauthorized access to, use of, disclosure of, interruption of, alteration of, or deletion of information. To protect the data, code, and information that businesses collect from their clients and users, information security is employed.
3. Network Security: A network is secured against attacks and illegal access. It is the duty of network administrators to take security steps to shield their networks from potential dangers. An element of IT security is network security, which is a means to safeguard computer networks and prevent unauthorized access.
4. Business continuity planning/ Disaster recovery planning: Planning for disaster recovery or business continuity is the procedure that specifies how to resume operations efficiently after a disaster. The first step in creating a disaster recovery strategy should be to identify the apps that are normally crucial to running the business. Business continuity planning (BCP) links being prepared for cyber risk by detecting threats to the organization's schedule, understanding how potential disruptions to operations can influence them, and deciding how to deal with those disruptions.
5. Operational Security: In order to secure sensitive data from various dangers, managers are encouraged to view operations from the perspective of a hacker as part of a process known as operational security (OPSEC) or procedural security. An association's operations are protected using operations security (OPSEC). It keeps track of essential data and resources to spot any weaknesses in the practical technique.
6. End User Education: End-user training is the most critical component of computer security. End users are transforming into the greatest security danger in any relationship since it can happen at whatever point. One of the essential blunders that lead to data breaks is human mix-ups. An affiliation ought to set up its labourers about network protection. Every delegate ought to realize about phishing assaults through messages and connection points and might perhaps oversee digital risks (swarnavo09, 2022).

Challenges and Threats to Cybersecurity in India

The amount of people with internet access is constantly growing in India. India is currently the world's second-largest internet market despite its unmet potential. Although the development of technology and the internet has all the associated advantages, it has also resulted in a rise in cybercrime that affects people all over the world. The Pegasus snooping scandal and the WannaCry attack have both highlighted how vulnerable India is to dangers from cybercrime. There are many risks and difficulties for India's cyber security:

1. Cyberterrorism: It is a planned, violent attack with political motivation against data, computer systems, programs, and information.
2. Digital data threat: Increasing online sales have given thieves more motivation. In addition to collecting data (such as customer information, the findings of product surveys, and general market intelligence), businesses often produce intellectual property, which is in and of itself a desirable objective.
3. Cyberwarfare: It is the act of a nation-state or international organization attacking and attempting to compromise the computers or information networks of another country.
4. Cyber Infrastructure Concerns: Like any other connected system, most technology and equipment are susceptible to cyber threats. Despite creating the National Critical Information Infrastructure Protection Centre (NCIIPC), the government has not yet decided on and put protective measures in place for critical information infrastructure.

5. Lack of experts: According to Internet World Stats' 2017 report, India is the country with the second-highest number of Internet users worldwide, behind China. However, relative to the number of internet users, India has a very small population of cyber-security experts.
6. India's approach to cyber security: India has thus far been erratic and non-systematic due to a lack of effective law enforcement measures. Despite several organizations, laws, and programs, their execution has been far from satisfactory.
7. Lack of Coordination: Due to the existence of too many agencies with overlapping functions in the field of cyber security, coordination between these agencies is poor (Mains Marathon, n.d.).

Methods of Attack and Avoidance

1. Phishing: One of the frequent cybercrimes used to attack targets is phishing. The hackers send the targets phishing emails using this technique. These emails offer the appearance that they are coming from a reliable source or a well-known individual. These phishing emails often even include attachments to trick the receiver.
2. Malware: Malicious software, sometimes known as malware, is employed to harm other computer systems. Ransomware, viruses, worms, and spyware are a few types of malwares. When you open an attachment or click a dubious link, the virus will be downloaded and installed on your computer. The software causes mayhem once it has been installed on your PC.
3. Denial-of-Service: A cyberattack known as a DoS floods a website or application with artificial traffic that is greater than it can handle. Once this assault is initiated, authorized users won't be able to access the website or application. There could be a number of causes for this kind of attack. It might be done to force the victims to pay.
4. SQL Injection Attack: One of the most likely assaults, SQL Injection will be extremely harmful to enterprises. Through SQL injection, cybercriminals attack databases and commit crimes such as data deletion, corruption, modification, theft, and authentication bypassing, among others.
5. Drive-by Attack: In this attack, the hackers won't wait for a user action to infect their systems with malware. Instead, they include the harmful code in the PHP or HTTP code on a website or web application page. Now, whenever someone accesses that page that contains malicious code, the virus is downloaded and installed on their computer. The main targets of this form of assault are insecure websites or applications.
6. Password Attack: This is one of the most popular techniques for gaining unauthorized access to other systems on a network. The hackers sniff the connection between a system and a network or grab passwords from a person's desk as part of this assault. To randomly guess passwords, the hackers also employ the brute force technique. They try using the target's personal information, such as name, occupation, and job title, etc., to try and guess the password.
7. Man in the Middle (MITM) Attack: This type of attack places the hacker in the middle of the interaction between the user and the program. This assault aims to steal information from users of financial apps, websites, and eCommerce portals, etc., including login passwords, credit card information, account information, etc.
8. Eavesdropping Attack: This attack aims to intercept information being sent through a network or to any other connected device. Because the network seems to function perfectly regularly even when under attack, it is incredibly challenging to detect this attack. The hacker installs a sniffer on a server or system before launching this attack. The sniffer intercepts the transferred data after it is deployed.
9. Cross-site scripting (XSS) attack: In the XSS attack, the programmers embed outsider assets in the designated applications or the programs and debase the data set with vindictive JavaScript. During perusing, the malevolent JavaScript will be communicated to the guest's program as a component of the HTML body and gets executed. Utilizing this assault, the programmer can take treats and organization data, and so on (Sandeep, n.d.).

Need for Cybersecurity in India

In 9.4% of Indian homes, there is a computer (or workstation). The top three information/association domains with the most notable PC use are Chandigarh (U/T), Goa, and NCT of Delhi. In India, only 2.3 percent of all residences have access to the Internet, according to the 2018 Enumeration. Only 86,47,473 (3.3%) of the 34,66,92,667 (346.7 million) dwellings in India were counted during the enumeration. The Web incorporates both broadband and low-speed associations (Gupta, 2018).

As indicated by Web World Details on June 30 2012, there were 2.4 billion web clients (2,405,510,175) around the world. China was the biggest nations regarding web clients with north of 538 million clients (World Internet Users and 2023 Population Stats, 2022).

The following graph (figure 1) shows top 15 internet countries worldwide at mid-year 2018:

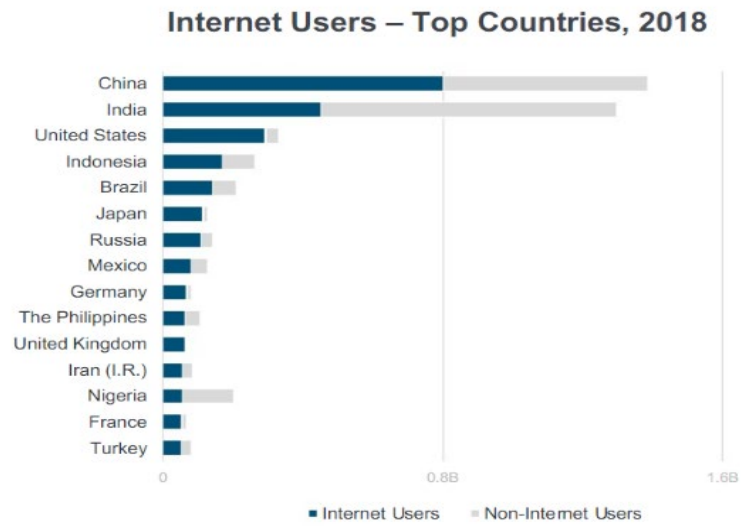

Figure 1. Top countries in the world by internet usage in 2018.
(Source: www.weforum.org)

Figure 2 of the following graph illustrates the expansion of e-commerce in India, which reached 39460 million USD in 2021.

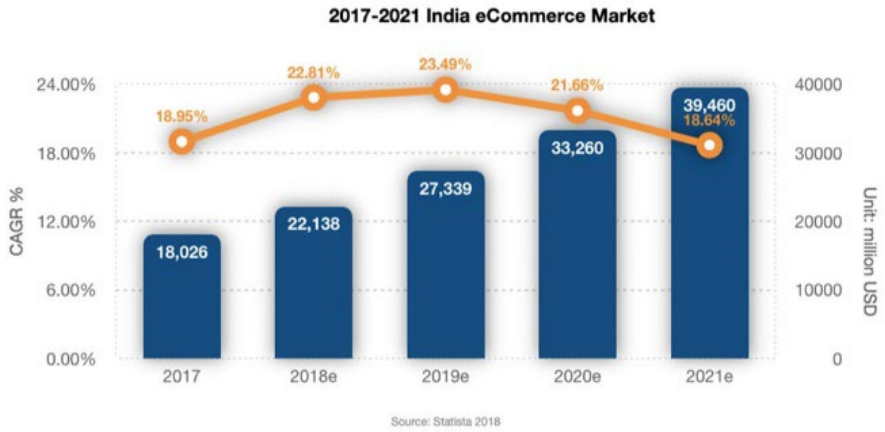

Figure 2. E-commerce usage is rising in India
(Source: www.indianretailer.com)

Nowadays, most purchases take place online. The increase in digital transactions in India is depicted in the graph below (figure 3). Digital payment transactions have been consistently increasing over the past few years as part of the Indian government's strategy to digitize the financial sector and economy.

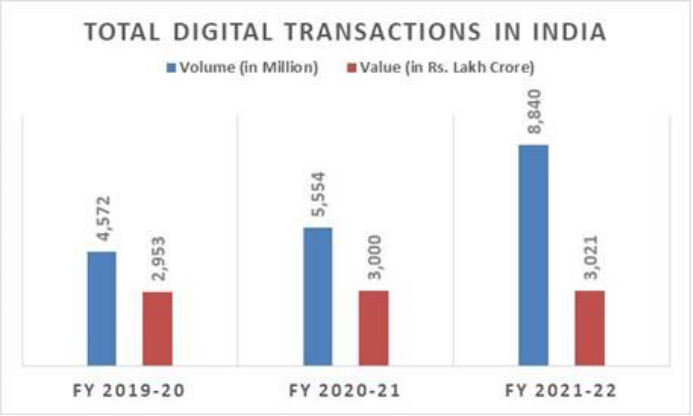

Figure 3. Total digital transactions in India FY 2019-2022
(Source: pib.gov.in)

With this multitude of figures, obviously India, a country that is quickly growing, especially in the fields of data innovation and web-based business, is fully on guard for online channel security to forestall extortion and monetary misfortunes.

The Worldwide Network Protection File (GCI) is a legitimate asset that surveys every country's commitment to online protection on a worldwide scale to feature the importance and scope of the issue. Since network protection has a large number of uses in numerous businesses and areas, every country's level of improvement or support is estimated along five support points - (i)Organizational Measures, (ii) Legitimate Measures, (iii) Specialized Measures, (iv) Participation, and (v) Limit Improvement - and afterward collected into a general score. (Sahu, 2021)

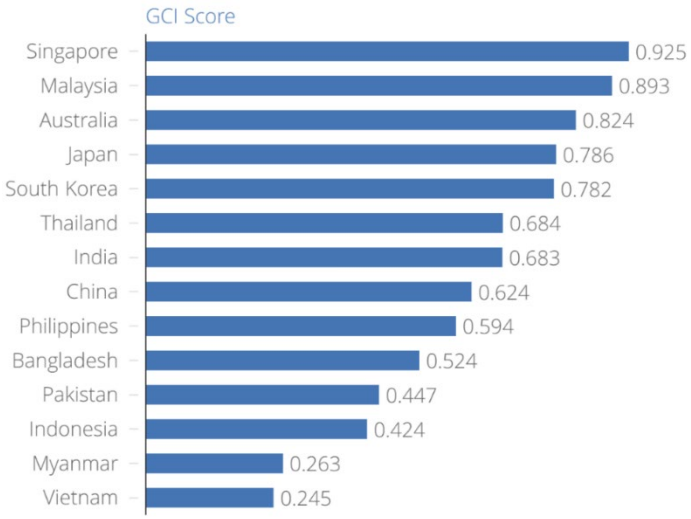

Figure 4. Global Cybersecurity index: Ranking of Asia-Pacific countries
(Source: www.brinknews.com)

UN network safety record 2017: India has been ranked 23rd among 165 nations by the Joined Countries worldwide digital protection list. In the Asia Pacific area, India takes the seventh spot (Global Cybersecurity Index, 2017).

The episodes of cybercrimes in India have been expanding at a quick speed and bounced by almost multiple times somewhere in the range of 2013 and 2020, official information showed. According to the most recent 'Wrongdoing in India' report, violations in India expanded to 50,035 during 2020 from 5,693 cases detailed in 2013. Further, according to the information investigated by CNN-News18, somewhere in the range of 2018 and 2020, the cases hopped by almost 85%. In 2018, India recorded 27,248 cases connected with cybercrime. Additionally, the cases announced in 2020 were almost 12% more than that kept in 2019 — 44,735 cases (Singh, 2021).

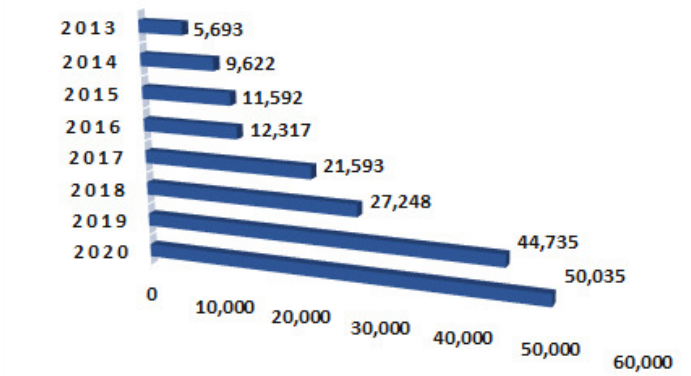

Figure 5. Cybercrime reported in India (Source: www.news18.com)
The main explanation is that we have a great deal of chances in light of the high speed of the business. Essentially, the main thing to find a new line of work ought to be the accessibility of chances. There is an

enormous interest in the business however the stockpile is less. Network safety is an enduring choice. Since, the interest for network safety experts is more than the inventory, it is a very much compensated calling. With the range of time, online protection isn't simply a centre innovation area yet it has likewise turned into a first rate prerequisite at the present situations (Choudhary, 2021).

It is crucial for India to give cybersecurity top priority due to the rising threat of cyberattacks and the country's growing reliance on digital technologies. By putting in place robust cybersecurity safeguards, India can defend its vital infrastructure, secure the privacy and data of its population, and guarantee the ongoing expansion of its digital economy.

Cybersecurity Initiatives in India

The greatest strategy to protect an organization's IT infrastructure in today's high-tech digital environment is to maintain proper cybersecurity measures. These dangers hurt government institutions in addition to corporations. The Indian government's implementation of cyber security measures would contribute to the maintenance of a safe online environment and reduce the hazards brought on by the threat.

- CERT-In: India's national cybersecurity organization, The Indian Computer Emergency Response Team (CERT-In), has improved the country's cybersecurity, which has resulted in a decrease in cyberattacks on government networks. Government workers in India are better equipped to combat cybercrime by training them on cybersecurity awareness and anti-phishing. The CERT-In Group not only raises awareness of the risks posed by phishing attempts but also updates the public on the most recent cyber vulnerabilities and defenses against them.
- Cyber Surakshit Bharat: The Service of Gadgets and Data Innovation (MeitY) sent off this program determined to foster areas of strength for an environment in India. This is predictable with the public authority's objective of making a "Computerized India." This program was upheld by the Public E-Government Division (NeGD).
- National Critical Information Infrastructure Protection Centre: India has laid out the Public Basic Data Framework Insurance Centre as a component of its network safety drives to safeguard indispensable data vital to general wellbeing, monetary turn of events, and public safety. The Data Innovation (IT) Demonstration of 2000 changed this statement in Area 70A. This association runs network safety drills to guarantee that the public authority and significant areas are prepared with regard to online protection.
- Cyber Swachhta Kendra: On August 28, 2019, New Delhi hosted the 12th India Security Summit, which had as its theme "Towards New National Cyber Security Strategy." The seminar covered a variety of themes, including defending vital national infrastructure and dealing with new cyber threats. It was also mentioned during the panel that cybersecurity is a difficult topic in the digital world, so new tools and technology need to be developed more swiftly.
- National Cyber Security Strategy 2020: A Public Digital Protection System 2020 is still being worked on at the Indian government network safety division Public Safety Committee Secretariat by the Workplace of the Public Network safety Facilitator. Data security alludes to forestalling assaults, harm, abuse, and monetary surveillance in the internet. A three-layered association, the Public Safety Gathering (NSC) of India regulates issues connected with governmental issues, the economy, energy, and security (Latest 10 Indian Government Initiatives on Cybersecurity, n.d.).

India's legal framework for Cybersecurity

1. The Information Technology Act of 2000: The first significant cybersecurity regulation in India was the Information Technology Act of 2000. The IT Act of 2000, passed by the Indian Parliament to direct cybersecurity legislation, set data protection standards, and prevent cybercrime, is enforced by the Indian Computer Emergency Response Team (CERT-In). It supports the private sector, internet shopping, online banking, among many other things.
2. Information Technology (Amendment) Act of 2008: The IT Act of 2008 expanded the definition of cybercrime and established the validity of electronic signatures. It also incorporated updated and redefined phrases for contemporary use. Additionally, it holds businesses accountable for data breaches and actively encourages them to establish better data security practices.
3. Information Technology Rules, 2011: The main changes concern the guideline of middle people, re-examined fines and punishments for offenses like cheating, defamation, and distributing private photos without assent, as well as the control/limitation of specific discourse.
4. Indian SPDI Rules, 2011, for Reasonable Security Practises: The Indian SPDI Rules, 2011, identify the IS/ISO/IEC 27001 norms as global standards. As a result, Indian businesses are not required to follow

these guidelines, but they are strongly encouraged to do so since they can assist them in adhering to the "reasonable security practices" required by Indian law.

5. National Cyber Security Policy, 2013: In order to help public and commercial organizations better defend themselves against cyberattacks, the Department of Electronics and Information Technology (DeitY) published the National Cyber Security Policy 2013 in 2013.
6. IT Rules, 2011: The Ministry of Electronics and Information Technology introduced the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 on February 25, 2021, to replace the IT Rules, 2011. The Indian MeitY (Ministry of Electronics and IT) has updated the draught modifications and published them in order to strengthen the IT Act and meet the demands of the rapidly evolving digital environment.
7. Reserve Bank of India Act 2018: The Reserve Bank of India introduced the RBI Act in 2018, which details cybersecurity guidelines and frameworks for UCBs (urban co-operative banks) and payment operators (Chin, 2023).

Findings

- There is a significant gap between the demand for cybersecurity professionals and the supply of qualified personnel in India.
- The Indian government has taken several initiatives to improve cybersecurity in the country.
- India is rapidly digitizing, with more people coming online and using digital services. This has led to an increase in cybersecurity threats, such as hacking, malware, and phishing attacks.
- Another issue is the low awareness of cybersecurity among the general public which is a major reason for cybercrimes.
- Overall, cybersecurity is an important issue for India to address as it continues to digitize and integrate into the global economy.

Conclusion

In conclusion, cybersecurity has become a major concern in India, with the rapid digitization of the country's economy and society. The increasing number of cyber-attacks and data breaches is a clear indication that more needs to be done to strengthen India's cybersecurity posture.

- Increase cybersecurity awareness and education: The Indian government should launch a national cybersecurity awareness campaign to educate citizens about the risks of cyber threats and how to protect themselves. This should include targeted outreach to vulnerable groups such as small and medium-sized businesses, schools, and individuals.
- Develop a comprehensive cybersecurity policy: India should develop a comprehensive cybersecurity policy that outlines a national cybersecurity strategy and establishes standards for cybersecurity across all sectors. The policy should also provide guidelines for incident response and recovery.
- Strengthen collaboration between the public and private sectors: The Indian government should work closely with the private sector to identify and mitigate cybersecurity risks. This could include creating public-private partnerships to develop cybersecurity solutions and establishing sector-specific cybersecurity working groups.
- Increase investment in cybersecurity research and development: India should increase investment in cybersecurity research and development to stay at the forefront of cybersecurity innovation. This would help ensure that India is equipped to address emerging threats such as AI-powered cyberattacks and quantum computing-based threats.
- Strengthen data protection regulations: India should strengthen data protection regulations to protect the privacy of citizens and businesses. This could include implementing strong data protection laws, ensuring compliance with international data protection standards, and promoting the use of encryption technologies.

India must be a part of international cooperation efforts to promote responsible behaviour in cyberspace. The country is still not a signatory to several conventions including the Budapest Convention (Council of Europe, n.d.), which it considers to be outdated and lop-sided. The convention includes other clauses like trans-border data access, which impinges on national security. Since India was not consulted at the time the Convention draft was made, leaning in favour of the Western Bloc, it is looking for a more balanced alternative. In the meanwhile, the Budapest Convention, which has been in effect for two decades, can be modernized and made more democratic by taking into account the issues facing the developing world, which will house the bulk of the world's future consumers.

References

Chin (2023, March 02), Top Cybersecurity Regulations in India. Retrieved from UpGuard: https://www.upguard.com/blog/cybersecurity-regulations-india

Chitra (n.d.), A brief analysis of cybercrime in India. Retrieved from Legal Service India: https://www.legalserviceindia.com/legal/article-5961-a-brief-analysis-of-cyber-crime-in-india.html

Choudhary (2021), Shortage of the cybersecurity workforce in India is 9% higher than the global average: RV Raghu. Retrieved from Express Computer: https://www.expresscomputer.in/security/shortage-of-the-cybersecurity-workforce-in-india-is-9-higher-than-the-global-average-rv-raghu/78520/

Council of Europe (n.d.), Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention

Dani (2022), A Literature Review on Cyber Security in Indian Context. Comput Eng Inf Technol, 11(6).

Global Cybersecurity Index (2017), Retrieved from ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Gupta K (2018), Importance of cybersecurity in India. International Journal of Engineering Research, 5(3), 27.

Hati (2016), Cyber Crime: A Threat to the Nation and its Awareness. International Journal of Advanced Research in Computer and Communication Engineering, 5(7).

Lakshmanan (2019), Literature review on Cyber Crimes and its Prevention Mechanisms. doi:10.13140/RG.2.2.16573.51684

Latest 10 Indian Government Initiatives on Cybersecurity (n.d.), Retrieved from Securium Solutions : https://securiumsolutions.org/latest-10-indian-government-initiatives-on-cybersecurity/

Mains Marathon (n.d.), (Stellar Digital pvt ltd) Retrieved from Forum IAS: https://blog.forumias.com/answereddiscuss-various-threats-and-challenges-to-cyber-security-in-india-what-initiatives-are-being-taken-by-the-government-to-enhance-cyber-security-in-india/

Mali .S (2018), ANALYSING THE AWARENESS OF CYBER CRIME AND DESIGNING A RELEVANT FRAMEWORK WITH RESPECT TO CYBER WARFARE: AN EMPIRICAL STUDY. International Journal of Mechanical Engineering and Technology, 9(2), 110-124.

Ms.Chithra M (n.d.), Legal Service India.

Narnolia N (n.d.), Retrieved from www.legalserviceindia.com: https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html

Phillips D (2022, April 16), Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379-398.

Sahu (2021), Scaler Topics Global Cybersecurity Index. Retrieved from Scaler Topics: https://www.scaler.com/topics/global-cybersecurity-index/

Sandeep (n.d.), Cyber Attacks and Preventions Methods. Retrieved from MindMajix: https://mindmajix.com/cyber-security-attacks

Singh N (2021), Cyber Crimes in India Spiked Nearly Nine Times Since 2013, UP Topped Chart. Retrieved from News18: https://www.news18.com/news/india/cyber-crimes-in-india-spiked-nearly-nine-times-since-2013-up-topped-chart-in-2020-data-4210703.html

Supriya S (2022), CYBER CRIMES IN INDIA: A CRITICAL ANALYSIS. International Journal of Mechanical Engineering, 7(6).

swarnavo09 (2022, June 16), Elements of Cybersecurity. Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/elements-of-cybersecurity/

World Internet Users and 2023 Population Stats (2022, June), (Miniwatts Marketing Group) Retrieved from Internet world stats: https://www.internetworldstats.com/stats.htm

